Pass the hash:

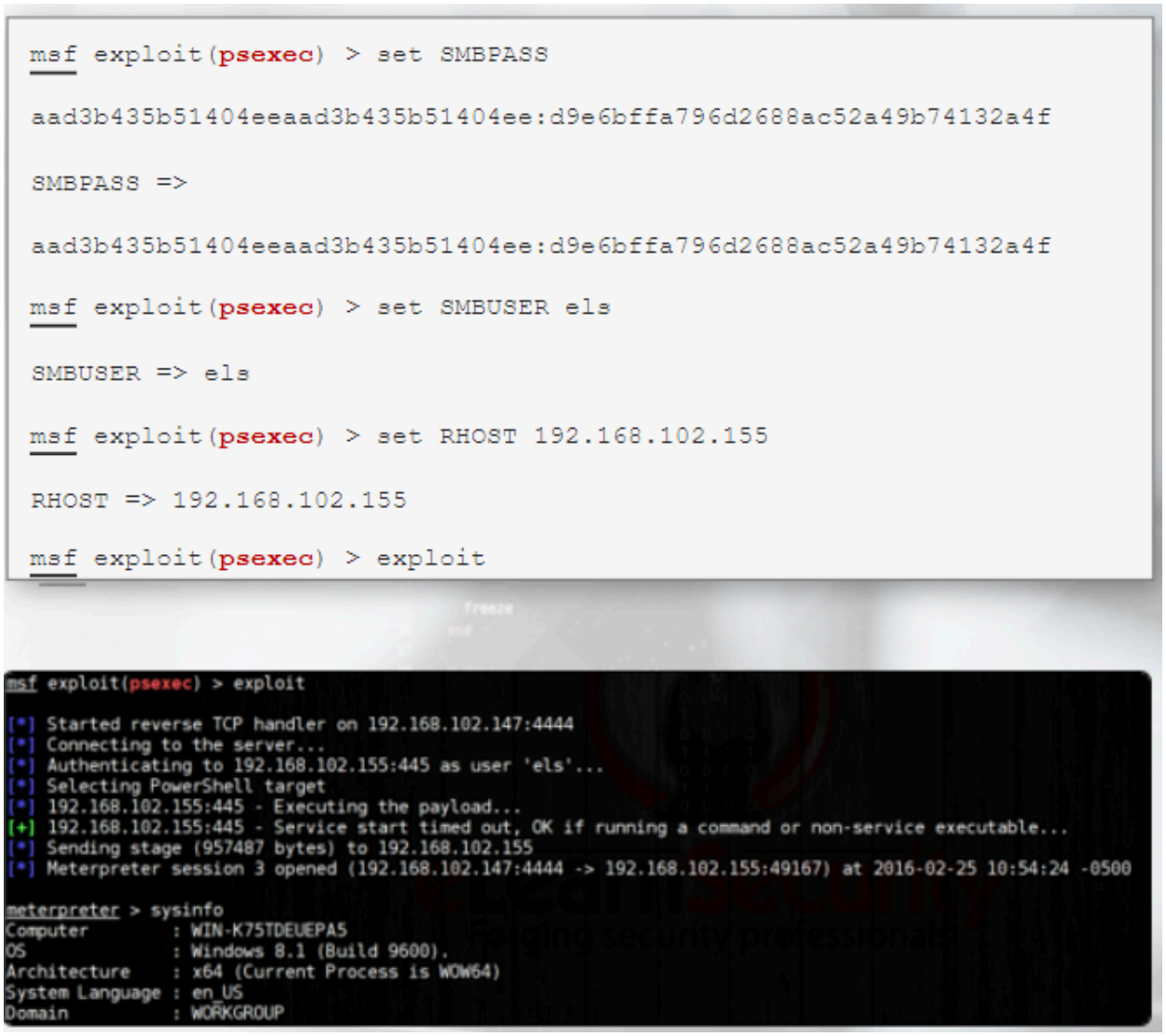
Here we will talk about the NTLM hashes. The NTLM hash is stored in the Security Account Manager (SAM) (registry hive) database in the host for local users authentication and also the user AD credentials are cached in the SAM and in domain controller the hash is stored in NTDS.dit which is used to verify the user credentials when the user try to login in the domain, this NTDS.dit file has the hash of all users in it, so accessing this file can be very helpful for the attackers.

with NTLM used for authentication the credentials of the AD users that used the Machine will be cached locally in the SAM hive, and the SAM is only accessible by admins, so attacker accessing the SAM in case of the NTLM being used, the credentials of this user can be extracted from the SAM

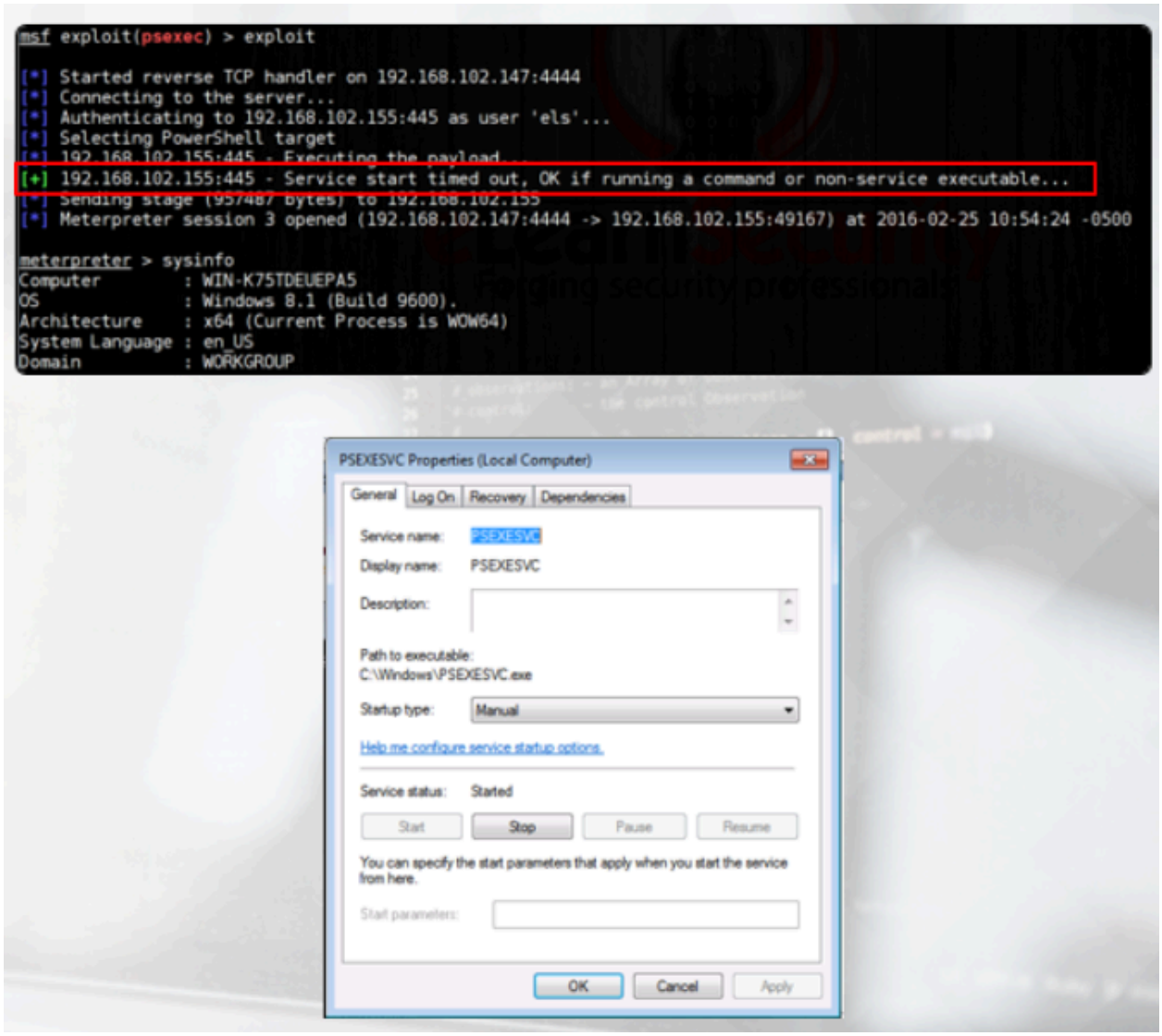
But the passwords hash of the NTLMv2 is not stored/cached on the system like the NTLM is stored on the system in SAM, with NTLMv2 its stored in the AD, mean not stored or cached locally.

When an attacker obtain the NTLM hash, they can perform an attack called “Pass the hash”, which will grant the access to the system they passed the hash to, mean without in need to have the plain-text password, it will just pass the hash to the target system and gain access to it. This can be used for lateral movement, to gain back access to a system and more …

There is many tools that can perform this “Pass the Hash” attack, attackers perform this attack usually through MetaSploit psexec module.



Here we see first the attacker provided the NTLM hash to the Metasploit, the username, then give it the target to that they want to perform the Pass The hash attack to which is RHOST or remote host and then exploit and got a shell in that target or remote shell.



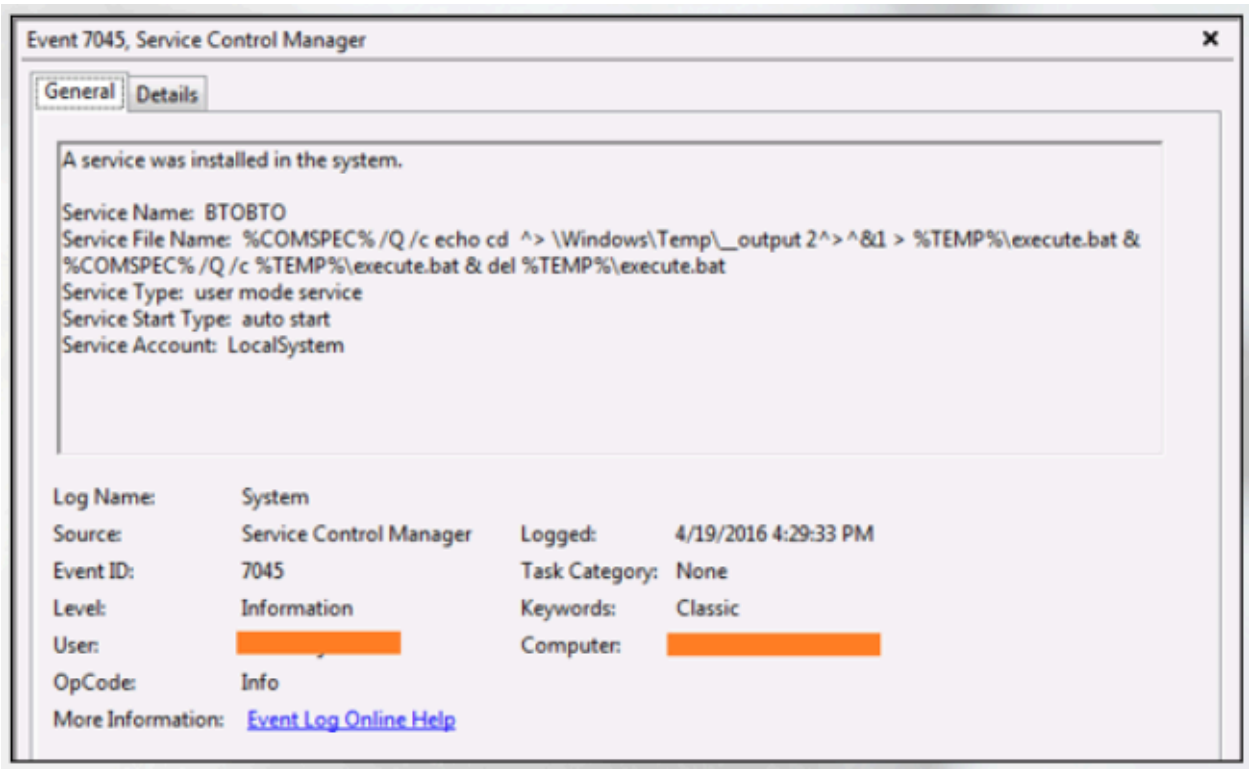
If we take a closer look at this psexec module we see it creates a service.

Specifically:

1. It copies a binary to the ADMIN$ share over SMB
2. It creates a service on the remote machine pointing to the abovementioned binary
3. It remotely starts the service
4. It stops the service and deletes the binary on exit

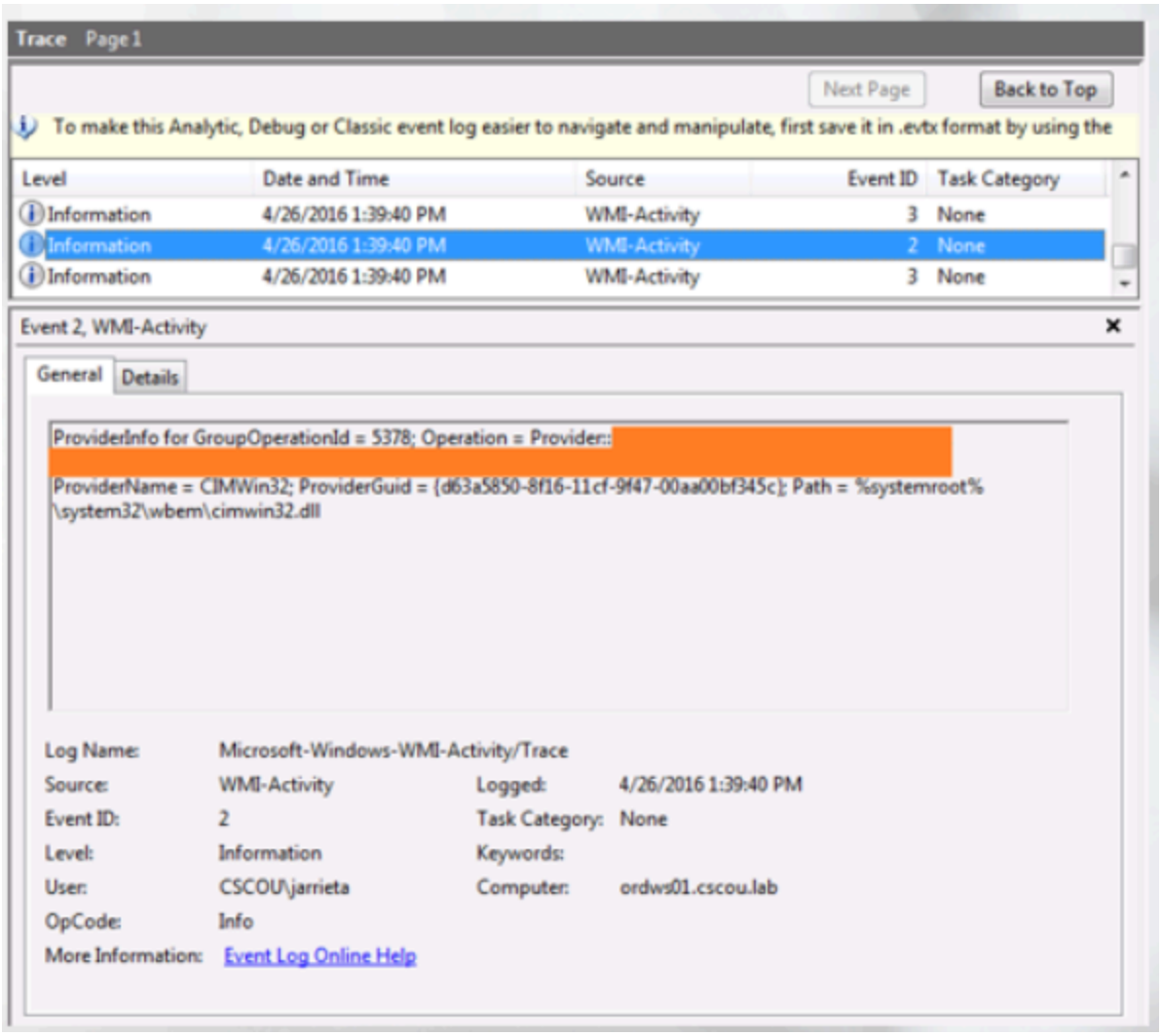
Newer tools like smbexec.py or the psexec it self can avoid dropping a binary on the disk, instead they can execute PowerShell commands through creating new services. For this on hosts we can use the event ID 7045 to check if a new service was created or installed, and if we have PowerShell block logging enabled, we can see the scripts and commands logged and even in Deobfuscated form.

ID 7045, new service installation logged:



Attackers can use WMI for the Pass the Hash attack where the attacker dosnt need to create a new service and no suspicious commands will be logged. For this, we need to enable the “Logging for WMI Events”, and its not enabled by default, so that’s why the suspicious command will not be logged.

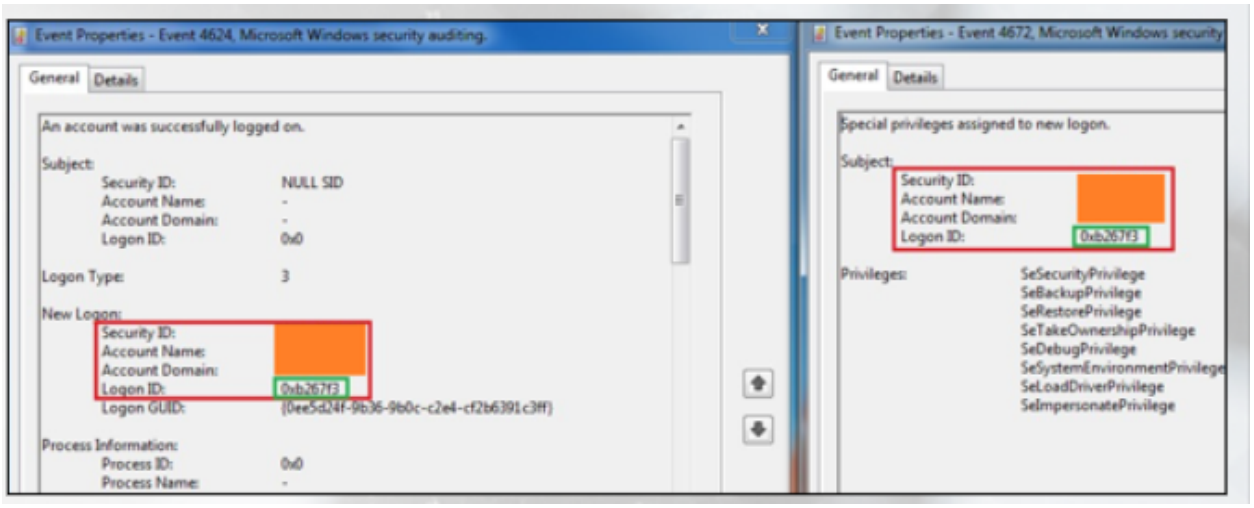
WMI activity:



We know that the Pass the Hash used for lateral movement and over the NTLM network, so there is NTLM connection involved.

So when an NTLM connections occurs for authentication, Event ID 4624 is logged which means successful login with Logon type being 3 which mean over the network.

To narrow things even more, we can focus on the privileged NTLM connection, and we can identify it by correlation of event ID 4672 and NTLM connection. So we check with NTLM connection if any user is logged in and then we check if any user when its logged got privileges with event 4672, mean when a user logs in remotely they will not have the privileges, but if the machine is configured to allow it, first the user logs in and then it will be assign the privileges.(thats how the remote logins works in windows)


Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
An account was successfully logged on.
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Type: 3
New Logon:
Security ID:
Account Name:
Account Domain:
Logon ID: 0xb267f3
Logon GUID: {0ee5d24f-9b36-9b0c-c2e4-cf2b6391c3ff}
Process Information:
Process ID: 0x0
Process Name: -
Event Properties - Event 4672, Microsoft Windows security
General
Details
Special privileges assigned to new logon.
Subject:
Security ID:
Account Name:
Account Domain:
Logon ID: 0xb267f3
Privileges: SeSecurityPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeTakeOwnershipPrivilege
SeDebugPrivilege
SeSystemEnvironmentPrivilege
SeLoadDriverPrivilege
SeImpersonatePrivilege